Institutional Repository - Research Portal
Dépôt Institutionnel - Portail de la Recherche
researchportal.unamur.be
University of Namur

RESEARCH OUTPUTS / RÉSULTATS DE RECHERCHE

A propos du sommet mondial sur la société de l'information. Les ambiguïtés de la gouvernance de l'Internet

Dumortier, Franck

Published in:
Revue du Droit des Technologies de l'information

Publication date:
2006

Document Version
le PDF de l'éditeur

Link to publication

Citation for pulished version (HARVARD):
Dumortier, F 2006, 'A propos du sommet mondial sur la société de l'information. Les ambiguïtés de la gouvernance de l'Internet', *Revue du Droit des Technologies de l'information*, Numéro 25, p. 143-168.

General rights
Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
- You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the URL identifying the publication in the public portal ?

Take down policy
If you believe that this document breaches copyright please contact us providing details, and we will remove access to the work immediately and investigate your claim.

Download date: 04. May. 2023

DOCTRINE

À propos du Sommet mondial sur la société de l'information

Les ambiguïtés de la gouvernance de l'Internet

Franck Dumortier[1]

Introduction

À l'issue de la première phase du Sommet mondial sur la société de l'information[2] (SMSI) en décembre 2003, les États ont adopté une Déclaration de principes[3] et un Plan d'action[4] établissant un Groupe de travail sur la gouvernance de l'Internet[5] (GTGI) chargé d'étudier la question de la gouvernance de l'Internet.

Conformément à son mandat, le GTGI a formulé une «définition de travail» de cette notion dans son rapport[6] de juin 2005:

«*Il faut entendre par 'gouvernance de l'Internet' l'élaboration et l'application par les États, le secteur privé et la société civile, dans le cadre de leurs rôles respectifs, de principes, normes,*

1. Chercheur au CRID. L'auteur remercie Séverine Dusollier, Cécile de TERWANGNE et Yves POULLET, ainsi que Yorick COOL et Virginie FOSSOUL, pour leurs relectures approfondies et leurs commentaires pertinents.
2. Aux termes de sa Résolution 56/183 (21 décembre 2001), l'Assemblée générale de l'ONU a approuvé la tenue du Sommet mondial sur la société de l'information (SMSI) en deux phases, dont la première a eu lieu à Genève (Suisse), du 10 au 12 décembre 2003, et la seconde à Tunis (Tunisie), du 16 au 18 novembre 2005. L'objectif de la première phase était le suivant: formuler de façon parfaitement claire une volonté politique et prendre des mesures concrètes pour poser les bases d'une société de l'information accessible à tous, tout en tenant pleinement compte des différents intérêts en jeu. L'objectif de la deuxième phase consistait à mettre en œuvre le Plan d'action de Genève et à aboutir à des solutions et parvenir à des accords sur la gouvernance de l'Internet, les mécanismes de financement, le suivi et la mise en œuvre des documents de Genève et Tunis. Pour plus d'informations, voy. <http://www.itu.int/wsis/index-fr.html>.
3. Déclaration de principes du SMSI, ref WSIS-03/GENEVA/DOC/0004, disponible sur <http://www.itu.int/wsis/docs/geneva/official/dop-fr.html>.
4. Plan d'action du SMSI, ref WSIS-03/GENEVA/DOC/0005, disponible sur <http://www.itu.int/wsis/docs/geneva/official/poa-fr.html>.
5. Le GTGI a été créé en octobre 2004 par le Secrétaire général de l'ONU. Ses membres ont été élus dans une liste de noms fournie par les gouvernements, les institutions civiles, le secteur privé et les institutions internationales et multilatérales, l'ONU conservant le dernier mot sur l'élection définitive des participants.
6. Rapport final du Groupe de travail sur la gouvernance de l'Internet, juin 2005, disponible sur http://www.wgig.org/docs/WGIGReport-French.doc.

règles, procédures de prise de décisions et programmes communs propres à modeler l'évolution et l'utilisation de l'Internet».

Ce rapport s'empresse de préciser qu'«*il faut bien comprendre toutefois que la gouvernance de l'Internet recouvre davantage que la gestion des noms et adresses utilisés dans le réseau mondial et les questions dont s'occupe l'Internet Corporation for Assigned Names et qu'elle englobe aussi des questions de politique générale importantes, comme les ressources Internet critiques, la sécurité et la sûreté du réseau mondial et ce qui touche à son développement et à l'utilisation qui en est faite*»[7].

Tant la définition fonctionnelle que le champ d'application très large de la notion eurent pour conséquence que, dans l'esprit du GTGI et dans le cadre des débats qui ont suivi son rapport lors du Sommet de Tunis, la «gouvernance de l'Internet» a englobé non seulement les questions de gestion des protocoles, des noms de domaine, des serveurs de noms et des adresses IP (gouvernance de l'Internet au sens strict), mais également toute une série de problématiques moins «structurelles» liées aux usages de l'Internet, telles que la cybercriminalité, le *spam*, l'accès universel, la propriété intellectuelle, la liberté d'expression, le multilinguisme, les droits des consommateurs, la protection de la vie privée, la concurrence, *etc.*, ce que nous appelons la gouvernance de l'Internet au sens large.

Ces deux types de considérations sont cependant de nature extrêmement différente. Selon nous, une distinction claire entre «gouvernance de l'Internet au sens strict»[8] et «gouvernance de l'Internet au sens large»[9] aurait eu pour avantage de clarifier les débats lors des négociations de Tunis.

Un argument majeur plaide toutefois en faveur d'une définition large de la gouvernance. En effet, l'Internet étant par essence «international», un cadre décisionnel global relatif aux seuls aspects techniques liés à l'infrastructure fondamentale de l'Internet semble insuffisant; nombre de questions d'intérêt général nécessitent également un traitement international en raison de l'impuissance des États, par essence territoriaux, à réguler de manière «nationale» un espace de communication ouvert créé pour l'échange transfrontière d'informations. Par ailleurs, la nature «ouverte» de l'Internet empêcherait un découpage de cet espace global en plus de 200 territoires «souverains» régulés par des lois et politiques différentes.

Si l'on accepte le postulat selon lequel l'étendue de la notion de «gouvernance» dépend des caractéristiques de la réalité appelée à être régulée, le champ large de la définition de «la gouvernance de l'Internet» résulterait d'une conception de l'architecture extrêmement distribuée, partagée, non hiérarchisée et non centralisée de l'Internet.

7. *Ibid*.
8. La «gouvernance de l'Internet au sens strict» peut être définie comme étant «*l'élaboration et l'application par les acteurs concernés, chacun selon son rôle, de principes, normes, règles, procédures de prise de décision et programmes communs propres à modeler, spécifiquement, la coordination et la gestion des ressources fondamentales de l'Internet*».
9. Dans le même esprit, la «gouvernance de l'Internet au sens large» peut être définie comme étant «*l'élaboration et l'application par les acteurs concernés, chacun selon son rôle, de principes, normes, règles, procédures de prise de décision et programmes communs propres à modeler l'évolution et l'utilisation de l'Internet, à l'exception de la coordination et la gestion des ressources fondamentales de l'Internet*».

Ces caractéristiques structurelles requerraient, par conséquent, des mécanismes de gouvernance dans lesquels l'ensemble des acteurs privés, publics et civils impliqués élaborent et appliquent des normes dans leurs divers champs de compétence respectifs. Cette multitude de champs de compétence expliquerait enfin la quantité de matières englobées par la notion.

Néanmoins, nous relèverons que la conception de l'Internet en tant qu'infrastructure non hiérarchisée et non centralisée néglige le fait que le *réseau des réseaux* a un point de contrôle unique. Dans un premier temps, nous examinerons donc l'importance de DNS[10] et décrirons brièvement sa réalité technique (chap. 1).

Conformément au postulat présenté ci-dessus, nous porterons ensuite notre attention sur les principes et mécanismes de «gouvernance au sens strict» mis en place actuellement pour gérer l'espace de nommage et les serveurs de noms racine (chap. 2).

Dans un troisième temps, nous dénoncerons la trop classique distinction entre questions «techniques» et considérations «politiques» dans le discours relatif à la «gouvernance au sens strict», en mettant particulièrement l'accent sur les implications «politiques» des problématiques d'inclusion et de re-

délégation des noms de domaine correspondant à des codes pays (chap. 3).

Enfin, grâce aux enseignements que nous aurons pu tirer de ces développements, nous exposerons en quoi la définition et le champ d'application larges donnés par le GTGI à la notion de gouvernance paraissent inadéquats pour élaborer, conformément aux termes du Plan d'Action de Genève, une «*position commune des rôles et des sphères de responsabilité respectives des gouvernements, des organisations intergouvernementales, des organisations internationales et des autres forums existants, ainsi que du secteur privé et de la société civile*»[11] (chap. 4).

En effet, la définition large et fonctionnelle de la gouvernance de l'Internet, telle qu'adoptée par le GTGI, a eu, selon nous, pour conséquence de reléguer au second plan les problématiques d'adressage et de nommage. Nous démontrerons cependant que ces problématiques essentielles sont loin d'être uniquement d'ordre technique et qu'elles ont des retombées non négligeables dans des matières relevant de la «gouvernance au sens large». Les rôles et les sphères de responsabilités respectives des divers acteurs en matière d'adressage et de nommage auraient donc dû, selon nous, être examinés en priorité.

10. Le Domain Name System (DNS) est le système d'annuaire mondial permettant d'associer des noms de machine/domaine (facilement mémorisables par des humains) à des adresses IP (utilisées par les machines pour communiquer entre elles).
11. Point 13, b), iii), du Plan d'action du SMSI, ref WSIS-03/GENEVA/DOC/0005, disponible sur <http://www.itu.int/wsis/docs/geneva/official/poa-fr.html>.

Chapitre 1
La réalité technique du DNS

1. L'importance du DNS

L'Internet peut être défini comme «*l'ensemble des interconnections d'hôtes – organisés en réseaux indépendants – qui, reliés par des liens de communication et des dispositifs de commutation, exploitent des protocoles standardisés afin d'échanger de l'information par le biais d'applications réseau*»[12]. D'un point de vue technique, le *réseau des réseaux* serait donc par essence extrêmement décentralisé et non hiérarchisé.

Aussi correcte soit-elle, cette description structurelle souffre cependant d'une faiblesse majeure en ce qu'elle minimise l'importance des applications réseau et protocoles assurant l'adressage et le nommage des différentes ressources disponibles sur la Toile.

Le DNS[13], mis au point[14] en juin 1983 par Paul Mockapetris, a précisément pour objectif de traduire les IP numériques en identifiants mnémotechniques appelés «noms de domaine». C'est à ce titre que ce système est d'une importance cruciale: les noms de domaine sont par exemple devenus la seule façon conviviale[15] de *se rendre* d'un site à un autre ou le seul moyen pour un logiciel de messagerie de savoir comment trouver le destinataire d'un message.

Tout en sachant que huit cent milliards de «requêtes DNS»[16] sont effectuées chaque jour[17], s'il est sans doute excessif d'affirmer que «*l'espace de nommage est Internet*»[18], il n'en reste pas moins que le DNS, en tant que «fonction coordonnée» au sein du *réseau des réseaux*, est l'une des pièces majeures qui doit être prise en compte sur l'échiquier de la gouvernance. Un ordinateur exclu de l'espace de nommage ou auquel une adresse IP n'est pas attribuée serait en effet concrètement banni de l'Internet car non adressable.

2. DNS: un système hiérarchisé

Tant au niveau de l'espace de nommage[19] qu'au niveau du système de serveurs de noms[20], DNS est, tout d'abord, un système hiérarchisé.

L'espace de nommage est en effet organisé comme une collection de bases de données partielles dans laquelle le rapport entre les domaines est soigneusement structuré. On parle souvent des noms de domaine selon leur niveau dans l'arbre: au sommet de la hiérar-

12. J. KUROSE, *Computer Networking: A Top-Down Approach Featuring the Internet*, 3e éd., mai 2004, p. 22.
13. Le DNS est un système comprenant deux composantes: d'une part, une base de données distribuée implémentée dans une hiérarchie de serveurs de noms; d'autre part, un protocole de niveau applicatif permettant aux hôtes et aux serveurs de noms de communiquer afin que le service de traduction puisse être fourni.
14. Tous les standards de l'Internet sont enregistrés en tant que RFCs (*Request for Comments*). DNS est décrit à l'origine dans les RFC 882 et RFC 883 et a ensuite été révisé en 1987 dans les RFCs 1034 et 1035. Le DNS a fait l'objet depuis de nombreuses RFCs.
15. Le protocole IP le permet également, mais il présente l'inconvénient de devoir taper de longues suites numériques.
16. Soit le fait de demander l'accès à un site Internet par le biais du nom de domaine de celui-ci.
17. G. CHATILLON, «L'internet: bien public, bien privé, bien commun», *Vox Internet 2005*, 30 juin 2005, p. 5.
18. H. KLEIN, *Icann et la gouvernance d'Internet*, document de réflexion pour l'Agence universitaire de la francophonie (AUF), p. 5, disponible sur <http://smsi.francophonie.org/IMG/pdf/icann-klein.pdf>.
19. C'est-à-dire la liste générale de paires «nom de domaine-adresse IP».
20. C'est-à-dire le support physique permettant l'exploitation de la base de données IP-noms de domaine.

chie, se trouve une zone unique: la racine (*root*); juste en dessous, se situent les «domaines de haut niveau»[21] (*top-level domains*, ou «TLD»); au niveau suivant, se trouvent des «domaines de deuxième niveau», et ainsi de suite.

Les machines appelées *serveurs de noms de domaine*, chargées d'établir la correspondance entre le nom de domaine et l'adresse IP des machines d'un réseau, sont également organisées de manière hiérarchique. Les serveurs correspondant au niveau hiérarchique le plus élevé sont appelés *serveurs de noms racine*. Leur rôle consiste à permettre de retrouver les adresses IP des serveurs DNS qui gèrent les domaines de premier niveau. Il en existe treize, répartis sur la planète, possédant les noms «a.root-server.net» à «m.root-server.net». De plus, les modifications apportées au fichier-zone racine ne peuvent l'être que via un *serveur racine caché* (*hidden master*), encore appelé *serveur racine de distribution* (*distribution master server*), dont la localisation géographique est maintenue secrète.

3. DNS: un système centralisé

Non seulement DNS est un système hiérarchisé, mais c'est également, *tel qu'il est implémenté*, un système centralisé, et ce à trois points de vue.

D'un point de vue technique, d'abord, l'espace de nommage doit se conformer, selon ses concepteurs, à certains principes: il doit notamment être unique[22], sous peine d'ôter toute fiabilité à l'adressage[23]. Il ne peut donc y avoir qu'une seule base de données contenant le listing de l'ensemble des paires nom-adresse IP; dans le cas contraire, «*deploying multiple public DNS roots would raise a very strong possibility that users of different ISPs who click on the same link on a web page could end up at different destinations, against the will of the web page designers*»[24]. Ce principe d'unicité de la racine (et donc de l'espace d'adressage) est, toujours d'après ses concepteurs, «*a technical constraint inherent in the design of the DNS*»[25], et non un choix politique[26].

21. Il existe trois catégories de TLD: les TLD génériques ou «gTLD» (.arpa, .com, .edu, .gov, .int, .mil, .net, .org, .name, .info, .coop, .pro); les TLD parrainés ou «sTLD», utilisés exclusivement par un secteur économique spécifique (.aero, .biz,...); enfin, les TLD en codes pays ou «ccTLD» (.be, .fr, .iq, .us, ...).
22. Internet Architecture Board, *IAB Technical Comment on the Unique DNS Root*, mai 2000, disponible sur <http://www.ietf.org/rfc/rfc2826.txt>. La nécessité d'une racine unique a été rappelée par l'ICANN dans son document ICP-3, *A unique, Authoritative root for the DNS,* 2001, disponible sur <http://www.icann.org/icp/icp-3.htm>.
23. M. MUELLER («Competing DNS Roots: Creative Destruction or JustPlain Destruction?», *Journal of Network Industries*, 20023(3), p. 2, disponible sur <http://istweb.syr.edu/~mueller/tprc-2001-mueller.pdf>) défend cependant l'idée que le principe d'unicité de la racine et de monopole sur celle-ci n'est en rien un postulat nécessaire. La fiabilité de l'adressage pourrait selon lui être assurée de manière équivalente dans un contexte de concurrence entre racines alternatives: «*One of the most intense and significant policy controversies associated with ICANN is the problem of competing DNS roots. Within Internet circles, the problem of competing roots has taken on the characteristics of a religious war. Internet 'Catholics', a collection of veteran techies acknowledging Vint Cerf as their Pope and the late Jon Postel as the Messiah, demand allegiance to The One True Universal Root. Internet Protestants, with elected ICANN Board member Karl Auerbach assuming the role of Luther, insist on the freedom to create alternate roots*». Ce point fait d'ailleurs l'objet de nombreux débats.
24. Internet Architecture Board, *IAB Technical Comment on the Unique DNS Root*, *op. cit.*
25. *Ibid.*
26. Selon M. MUELLER («Competing DNS Roots: Creative Destruction or JustPlain Destruction?», *op. cit.*, p. 2), un choix politique différent était possible: «*RFC 2826 confuses three distinct questions: 1) the factual issue of whether multiple roots can possibly exist; 2) the normative questions whether alternate roots should exist; i.e., whether the risks and costs of incompatibility are less desirable than the value created; and 3) the practical question of what is the appropriate policy response to alternate roots, once they do exist and a normative determination has been made*». De plus, des systèmes de racines alternatives existent déjà, même s'ils ne sont pas largement utilisés. Voy. p. ex.: ORSN (http://european.nl.orsn.net/), Cesidian Root (http://root.cyberterra.com/), Unified Root (http://www.unifiedroot.com/).

D'un point de vue géographique, ensuite, neufs serveurs racine «originaux», ainsi que le «serveur racine de distribution», sont gérés par des organismes américains[27].

Enfin, d'un point de vue organisationnel, le fichier-zone racine doit, selon ses concepteurs, être administré par une seule autorité: «*That one root must be supported by a set of coordinated root servers administered by a unique naming authority*»[28].

Si l'infrastructure de l'Internet a été conçue pour être décentralisée et distribuée, son fonctionnement demeure donc subordonné à une gestion centralisée du système technique d'adressage.

Chapitre 2
Les mécanismes de gouvernance au sens strict

1. Un modèle de gouvernance calqué sur le modèle technique

Le dernier point évoqué rappelle notre postulat introductif et révèle que la hiérarchie et la centralisation techniques de DNS influent également sur son modèle d'administration. La réalité hiérarchisée et centralisée de DNS déterminerait ainsi sa méthode de régulation propre, que l'on a dénommée plus haut la «gouvernance de l'Internet au sens strict».

Ainsi, conceptuellement, chaque domaine est non seulement doté d'une autorité directe l'administrant, mais est également, en raison de la hiérarchie technique, sous l'autorité indirecte de l'administration de niveau supérieur. Les différentes administrations fonctionnent selon la structure distribuée de l'espace de nommage: «*l'administration globale du DNS est une hiérarchie multi organisations, dans laquelle chaque administrateur exerce son contrôle sur les administrateurs des échelons inférieurs. Au sommet se trouve l'administrateur de la racine*»[29].

Dans le cadre de cette «régulation en cascade», l'administration de la racine est donc d'une importance toute particulière: «*L'autorité politique sur la racine – le pouvoir d'ajouter ou de supprimer les domaines de haut niveau – confère un contrôle direct sur tout domaine de haut niveau et un pouvoir indirect sur tout domaine de niveau inférieur*»[30].

2. Les acteurs de la gouvernance au sens strict

2.1. Les autorités administrative et politique de la racine

L'Internet Corporation for Assigned Names and Numbers (ICANN) fut créée

27. Pour des raisons propres au protocole DNS, le nombre de serveurs de noms racine ne peut être augmenté. Toutefois, la technique *anycast* permet de placer plusieurs répliques d'un même serveur, répondant à la même adresse IP, en différents endroits. À l'heure actuelle, cinq serveurs de noms racine (C, F, I, J et K) sont ainsi *anycastés*. Cependant, si cette technique permet de répartir géographiquement certains serveurs de noms racine, elle exige que toutes les répliques soient identiques et servent le même contenu; serveur original et répliques doivent donc être gérés par le même organisme.
28. Internet Architecture Board, *IAB Technical Comment on the Unique DNS Root*, *op. cit.*
29. H. KLEIN, *op. cit.*, p. 9.
30. *Ibid.*, p. 10.

en 1998[31] suite au Livre Blanc (ci-après « *White Paper* ») émis par le Département du Commerce des États-Unis (ci-après « DoC »)[32]. L'objectif *ostensible*[33] de cette initiative était de déplacer[34] la gestion des adresses IP et de la racine des noms de domaines des mains du gouvernement fédéral américain vers une organisation privée représentative de la « communauté Internet » au niveau international afin de soumettre l'espace de nommage à une certaine forme d'« autorégulation »[35], à l'abri de l'interventionnisme des gouvernements nationaux.

La teneur politique du *White Paper*[36] peut être résumée comme suit.

Dans un premier temps, est posé le postulat que l'organe ayant eu jusque-là l'autorité « technique » sur la racine est bien le gouvernement américain, sans quoi il n'aurait pas eu la légitimité nécessaire pour la transmettre[37].

Le gouvernement, se rendant compte qu'il n'a pas l'autorité requise en ce qui concerne la « gouvernance de l'Internet au sens large », souligne ensuite, sans doute par excès de conscience, que ce n'est finalement que le problème de l'adressage qui est visé.

Reprenant à son compte la nécessité présentée comme « technique » dans le RFC 2826, le DoC postule alors l'exigence d'une racine unique administrée par une seule entité à laquelle seraient transmises les compétences en matière d'adressage. Il soutient également que, pour des impératifs de « connectivité universelle » et de coûts, tous les moyens d'adressage (adresses et noms de domaines) doivent être concentrés entre les mains de la même entité. Enfin, pour des raisons dites de « coordination flexible », le gouvernement accepte que le processus de constitution de la nouvelle entité soit le fruit d'une certaine forme d'« autorégulation ».

31. L'objet de cette contribution n'étant pas de retracer l'historique de la formation de l'ICANN, nous nous limiterons à retracer son histoire depuis le *White paper*.
32. United States Department of Commerce, NTIA, *Management of Internet Names and Addresses*, Statement of Policy, Federal Register, vol 63, No 111, 5 juin 1998, 31741, disponible sur <http://www.icann.org/general/white-paper-05jun98.htm>.
33. Selon M. FROOMKIN («Wrong turn in cyberspace: using ICANN to route around the APA and the Constitution», *Duke Law Journal,* 2000, Vol 50:17, p. 70, disponible sur <http://personal.law.miami.edu/~froomkin/articles/icann.pdf>), «*The whole point of the White Paper had been to find a more formal structure for DNS management that left it in Postel's capable hands – and could be presented as a pro-Internet, deregulatory victory for the Clinton administration (and Ira Magaziner). ICANN exists because the Department of Commerce called for it to exist*».
34. United States Department of Commerce, NTIA, *Management of Internet Names and Addresses*, *op. cit.*
35. Notons que le concept d'«autorégulation» est susceptible de définitions diverses. Ainsi, dans le cadre communautaire européen, l'accord interinstitutionnel «Mieux légiférer» entend par «autorégulation», la possibilité pour les opérateurs économiques, les partenaires sociaux, les organisations non gouvernementales ou les associations, d'adopter entre eux et pour eux-mêmes des lignes directrices communes, notamment par des codes de conduite ou par des accords sectoriels (accord interinstitutionnel – «Mieux légiférer», 2003/C 321/01, *J.O.U.E.*, C 321 du 31 décembre 2003, pp. 1 et s., spéc. pt 22). Dans le contexte de DNS, l'administration Clinton s'est également réclamée, pour la création de l'ICANN, d'une approche «autorégulatrice». Il faut entendre par là que l'organisation, en tant que telle, ne serait pas créée par le gouvernement américain, pas plus que ses pouvoirs ou sa structure ne seraient spécifiquement définis par lui. Le secteur privé était au contraire invité à former l'organisation sur la base d'un large consensus entre les différents acteurs industriels concernés et à proposer une entité pouvant légitimement prétendre représenter la «communauté Internet». Le terme d'«autorégulation», dans ce contexte, désignait davantage une méthode de mise en place de la nouvelle entité qu'une méthode d'élaboration de règles dans un cadre institutionnel prédéfini. Il est à remarquer que ce concept d'«autorégulation» a été un leitmotiv de l'administration Clinton dans d'autres dossiers relatifs à l'économie numérique, et a dès lors caractérisé son approche dans les domaines de la télévision digitale, de la protection de la vie privée et de la régulation des contenus sur Internet. Voy. M. MUELLER, «ICANN and internet governance: sorting through the debris of 'self-regulation'», *Info* December 1999, Vol 1, No 6, p. 498, disponible sur <http://www.icannwatch.org/archive/ mueller_icann_and_internet_governance.pdf>.
36. United States Department of Commerce, NTIA, *Management of Internet Names and Addresses*, *op. cit.*
37. Cette «autorité originaire» américaine sur la racine est classiquement justifiée par le rôle historique des États-Unis dans le développement de l'Internet.

Deux limites sont cependant imposées aux acteurs concernés: d'une part, les acteurs industriels devront constituer la nouvelle entité sur le territoire américain, sans quoi la stabilité de l'Internet serait menacée; de l'autre, le gouvernement américain se réserve le droit de juger de la représentativité suffisante de la nouvelle entité avant de lui transmettre les compétences en matière d'adressage, révélant ainsi que la décision ultime dans le cadre du processus d'«autorégulation» revient en définitive au DoC.

Quelques mois après la publication du *White Paper*, en septembre 1998, l'ICANN était légalement constituée sous la forme d'une société à but non lucratif soumise au droit californien[38].

Si, en raison de ses compétences, l'ICANN peut incontestablement être perçue comme exerçant une parcelle d'autorité sur la racine, le *White Paper* révèle également que le DoC a insufflé à la gestion de la racine certaines positions propres qui ont significativement influencé la conception de l'administration de DNS. Dans la présente section, nous exposerons trois autres instruments juridiques qui confortent l'idée que le DoC peut être considéré comme étant l'autorité politique gouvernant le fichier-zone racine ainsi que le serveur primaire de distribution. Nous examinerons ainsi le protocole d'accord avec l'ICANN[39], le contrat relatif aux fonctions IANA[40] et, enfin, l'accord de coopération conclu avec VeriSign[41].

2.2. Les accords contractuels régissant la racine

2.2.1. Le protocole d'accord entre le DoC et l'ICANN

L'ICANN constituée, encore fallait-il que le gouvernement américain formalise le transfert des compétences qui seraient dévolues à la nouvelle entité. En novembre 1998, la jeune société conclut un «Memorandum of Understanding»[42] (ci-après «MoU») avec le DoC dans lequel l'ICANN était reconnue comme l'entité privée mentionnée dans le *White Paper*: «*(ICANN is) the organization that best demonstrated that it can accommodate the broad and diverse interest groups that make up the Internet community*»[43].

Néanmoins, avant de procéder au transfert intégral des tâches annoncé dans le *White Paper*, le DoC voulut s'assurer que le secteur privé avait la capacité et les ressources nécessaires afin d'en assumer les importantes responsabilités. À cette fin, le protocole d'accord prévoit une période transitoire au cours de laquelle l'ICANN est

38. Sans vouloir entrer dans un quelconque débat politique quant à la légitimité du processus ayant mené à la création de l'ICANN, l'on peut néanmoins relever que l'«autorégulation» revendiquée par l'administration américaine se rapproche conceptuellement bien plus dès le départ de la corégulation, «*mécanisme par lequel un acte législatif confère la réalisation des objectifs définis par l'autorité législative aux parties concernées reconnues dans le domaine*» (Accord interinstitutionnel – «Mieux légiférer», 2003/C 321/01, *J.O.U.E.*, C 321 du 31 décembre 2003, pp. 1 et s., spéc. pt 18). Les négociations passionnées dont a fait l'objet le *White Paper* démontrent d'ailleurs avec force la place prise par l'autorité politique dans la définition des objectifs.

39. Memorandum of Understanding entre le DoC et l'Icann, 25 novembre 1998, disponible sur <http://www.ntia.doc.gov/ntiahome/domainname/icann-memorandum.htm>. Cet accord a été amendé à plusieurs reprises. Les amendements sont disponibles sur <http://www.ntia.doc.gov/ntiahome/domainname/icann.htm>.

40. Contrat entre l'ICANN et le gouvernement américain en ce qui concerne l'exercice des «fonctions IANA», 9 février 2000, disponible sur <http://www.icann.org/general/iana-contract-09feb00.htm>. Ce contrat a été renouvelé en 2003 et modifié à plusieurs reprises. Ces modifications sont disponibles sur <http://www.ntia.doc.gov/ntiahome/domainname/iana.htm>.

41. L'accord de coopération entre le DoC et VeriSign (Network Solutions) et ses divers amendements sont disponibles sur <http://www.ntia.doc.gov/ntiahome/domainname/nsi.htm>.

42. Memorandum of Understanding entre le DoC et l'Icann, *op. cit.*

43. *Ibid.*

tenue de développer, en collaboration avec le DoC, les mécanismes, les méthodes et les procédures qui doivent être mises en place afin de gérer les principales fonctions DNS.

Ce qui, par écrit, semblait n'être qu'un stade temporaire, durant lequel le DoC «co-monitorerait» l'adressage jusqu'à ce que l'ICANN ait fait la preuve de sa capacité à gérer les responsabilités de manière autonome, s'avéra rapidement être une mainmise de longue durée du DoC sur le DNS. Le MoU fut en effet amendé et prolongé à six reprises, et ne pourra d'ailleurs être renégocié dans le futur qu'en septembre 2006. Quant à la preuve que doit faire l'ICANN de sa capacité à être autonome, le gouvernement américain de 1998 s'est sagement abstenu d'en fixer les critères d'évaluation objectifs et précis. Ce qui revient à dire, très concrètement, que l'ICANN ne sera reconnue autonome par le gouvernement américain que lorsque celui-ci le voudra bien.

S'agissant du contenu de ce protocole d'accord, le document et ses amendements mettent à charge de l'ICANN un certain nombre de tâches et de priorités permettant au DoC d'imposer ses positions en matière d'introduction de nouveaux TLD, de concurrence et de protection de la vie privée dans la base de données WHOIS[44], ainsi qu'en matière de relations avec les gestionnaires de ccTLD. Dans le cadre de cette «corégulation transitoire», la définition des objectifs et des priorités demeure donc du ressort du gouvernement américain; seule la réalisation de ces objectifs est déléguée au secteur privé. Cet instrument démontre une première fois que le DoC peut être considéré, encore actuellement, comme l'entité exerçant une certaine autorité politique sur la racine des noms de domaine.

2.2.2. Le contrat IANA

Le cadre des relations entre l'ICANN et le DoC ayant été fixé par le MoU, la société de droit californien a ensuite conclu un accord[45] avec le DoC concernant le transfert des fonctions «techniques» anciennement exercées par l'IANA[46].

Ces «fonctions IANA» recouvrent essentiellement l'allocation de blocs d'adresses IP aux Registres Internet Régionaux (RIR)[47], les activités administratives associées à la gestion de la racine, y compris la désignation d'administrateurs[48] lors de délégations[49] et de re-dé-

44. Annuaire permettant de rechercher l'existence d'un nom de domaine ou de l'information sur celui-ci. Le résultat de la recherche est soit la disponibilité du nom de domaine recherché, soit les informations sur le nom de domaine, telles que le nom et l'adresse du titulaire, les contacts administratifs, techniques et de facturation…
45. Contrat entre l'ICANN et le gouvernement américain en ce qui concerne l'exercice des «fonctions IANA», 9 février 2000.
46. Sigle de «Internet Assigned Numbers Authority». Un des organismes fondamentaux de l'Internet qui indexe de nombreuses données relatives à l'état du développement du réseau. Par ex., c'est l'IANA qui conserve la base de données des adresses IP encore libres sur le réseau. Pour plus d'informations, voy. <http://www.iana.org>.
47. Un Registre Internet Régional (RIR, de l'anglais *Regional Internet Registry*) alloue les adresses IP dans sa zone géographique. La politique d'allocation d'adresses IP, ainsi que la tarification, dépendent du RIR. Il existe aujourd'hui cinq RIR, regroupées dans le NRO (Number Resource Organization): APNIC (Asia Pacific Network Information Center), pour l'Asie et le Pacifique; ARIN (American Registry for Internet Numbers), pour l'Amérique du Nord; LACNIC (Latin American and Caribbean IP address Regional Registry), pour l'Amérique latine et les îles des Caraïbes; RIPE-NCC (Réseaux IP Européens), pour l'Europe et le Moyen-Orient; Afrinic, pour l'Afrique.
48. Contrat entre l'ICANN et le gouvernement américain en ce qui concerne l'exercice des «fonctions IANA», 13 mars 2003, sect. C.2.1.1.2, disponible sur <http://www.ntia.doc.gov/ntiahome/domainname/iana/2003/ianaorder_03142003.htm>.
49. La délégation des portions de l'espace de nommage appelées *top-level domains* consiste en la sélection d'un administrateur désigné pour un domaine capable de faire un travail équitable, juste, honnête et efficace. Ces autorités désignées constituent les administrateurs pour le domaine délégué et ont le devoir de servir la communauté. L'administrateur désigné est l'administrateur du top-level domain pour la nation et toute la communauté Internet.

légations[50], ainsi que la coordination des protocoles et des paramètres techniques. Il s'agit donc des fonctions «administratives» principales en matière d'adressage grâce auxquelles ordinateurs et humains peuvent communiquer sur l'Internet.

Ce contrat est important à deux niveaux pour notre propos. D'une part, il interdit à l'ICANN de procéder à l'édition du fichier-zone racine lors de délégations et de re-délégations[51]. Cela signifie que l'organisation privée n'est pas *matériellement* compétente pour modifier, ajouter ou supprimer des informations dans le serveur-racine de distribution (nous verrons *infra* que cette compétence revient à VeriSign). D'autre part, il interdit à l'ICANN de modifier les procédures et politiques établies qui guident l'exercice des fonctions IANA[52]. En ce qui concerne ses fonctions, l'organisation privée doit en effet respecter les procédures élaborées par le DoC et l'ICANN dans le cadre de la «corégulation transitoire» prévue par le MoU.

Par ailleurs, il n'est pas sans intérêt de relever qu'en vertu de ce contrat renouvelé en 2003, le DoC peut non seulement mettre fin unilatéralement à la délégation de compétences en cas de manquement par l'ICANN à ses obligations[53] et en cas d'absence de garanties de performances futures, mais qu'il peut également le faire de manière discrétionnaire[54] à sa seule convenance[55].

2.2.3. L'accord de coopération avec VeriSign

Pour ce qui est du système de serveurs de noms, il n'est pas sans conséquence de relever que VeriSign[56] a conclu un accord avec le DoC qui l'autorise à exploiter le serveur-racine A[57] ainsi que le «serveur racine de distribution», seul à contenir le fichier-zone racine original «éditable». Cet accord rend Versisign *matériellement* compétent pour l'édition du fichier-zone racine.

Il s'agit de l'instrument par excellence par lequel le DoC a affirmé explicitement son autorité sur toute modification du fichier-zone racine, ce qui apparaît clairement dans le passage suivant de cet accord: «*While NSI continues to operate the primary root server, it shall request written direction from an authorized USG official before making or rejecting any modifications, additions or deletions to the root zone file*»[58].

Bien plus que le MoU ou le contrat IANA, le contrat entre le DoC et VeriSign doit dès lors être considéré comme étant la principale source de l'autorité du DoC sur la racine. En effet, une mo-

50. La re-délégation des portions de l'espace de nommage appelées *top-level domains* concerne le processus de changement de l'administrateur désigné du ccTLD.
51. «*This purchase order, in itself, does not authorize modifications, additions, or deletions to the root zone file or associated information that constitute delegation or re-delegation of top level domains*» (contrat entre l'ICANN et le gouvernement américain en ce qui concerne l'exercice des «fonctions IANA», *op. cit.*, sect. C.2.1.1.2 et C.4.1).
52. Contrat entre l'ICANN et le gouvernement américain en ce qui concerne l'exercice des «fonctions IANA», *op. cit.*, sect. C.4.2.
53. *Ibid.*, sect. I, 1.
54. *Ibid*.
55. En ce qui concerne le mode de régulation, l'on peut dès lors se demander si de telles facultés réservées au DoC permettent réellement d'avoir recours au concept d'«autorégulation», voire de «corégulation».
56. Société commerciale américaine, principal opérateur du système des noms de domaine mondial, gestionnaire des extensions de haut niveau les plus lucratives (.com et .net).
57. Amendement 11 à l'accord de coopération entre le DoC et Verisign (Network Solutions), octobre 1998, disponible sur <http://www.ntia.doc.gov/ntiahome/domainname/proposals/docnsi100698.htm>.
58. *Ibid.*

dification du fichier-zone préalablement validée par l'ICANN doit encore recevoir l'aval du DoC avant que VeriSign puisse enfin, *matériellement*, éditer le fichier-racine au sein du serveur de distribution. En matière de délégation et de re-délégation, ainsi que lors de toute édition du fichier-zone racine, ce document octroie donc au DoC un droit de veto.

Ce cadre explique, par exemple, les pressions[59] et l'opposition exercées récemment par le DoC en vue de suspendre la création d'une extension .XXX pour les sites pornographiques, extension pourtant préalablement validée par l'ICANN.

Notons enfin que, le 30 juin 2005, le DoC a fait part de sa volonté de ne pas abandonner ce pouvoir de contrôle unique sur le fichier-zone racine[60].

Chapitre 3
Les implications politiques de la gouvernance au sens strict

1. La place des gouvernements nationaux dans la gestion du DNS

À l'origine du processus, le *White Paper*[61] déniait toute fonction décisionnelle aux gouvernements nationaux au sein de la nouvelle entité. Cette position résultait de la logique du choix politique originaire ayant mené à la création de l'ICANN: il a été conçu en tant qu'organisme «technique», non en tant qu'organe politique.

Si le *White Paper* ne réservait aucune place particulière aux gouvernements nationaux au sein de la nouvelle entité, tout rôle ne leur était pas dénié pour autant. Il était notamment stipulé que:

«*National governments acting as sovereigns… should (not) participate in management of Internet names and addresses (but will) continue to have, authority to manage or establish policy for their own ccTLDs*»[62].

Si le département américain a inclus cette exception dans le *White Paper*, c'est parce qu'il aurait été difficile de revendiquer une quelconque autorité sur les ccTLD, et ce déjà à l'époque de l'IANA. En effet, étant associés à un pays, ils relèvent par nature de l'autorité politique nationale. Aussi bien l'IANA que l'ICANN auraient été bien en peine de remettre en question le droit d'un gouvernement national à décider de sa politique publique dans l'environnement numérique. De plus, le

59. D. MCCULLAGH, «Noms de domaine: l'avenir du '.xxx' en suspens», *CNET News.com*, mardi 16 août 2005, disponible sur <http://www.zdnet.fr/actualites/internet/0,39020774,39252993,00.htm>.
60. «*The United States Government intends to preserve the security and stability of the Internet's Domain Name and Addressing System (DNS). Given the Internet's importance to the world's economy, it is essential that the underlying DNS of the Internet remain stable and secure. As such, the United States is committed to taking no action that would have the potential to adversely impact the effective and efficient operation of the DNS and will therefore maintain its historic role in authorizing changes or modifications to the authoritative root zone file*» (UNITED STATES DEPARTMENT OF COMMERCE, NTIA, *Domain Names: U.S. Principles on the Internet's Domain Name and Addressing System*, *op. cit.*).
61. United States Department of commerce, NTIA, *Management of Internet Names and Addresses*, *op. cit.*
62. *Ibid*.

White Paper étant le fruit d'âpres «négociations» au cours desquelles l'Union européenne avait fait valoir ses inquiétudes quant à l'approche excessivement centrée sur les États-Unis, cette exception était «politiquement» nécessaire.

Une certaine évolution quant à la place des gouvernements au sein de l'institution doit néanmoins être notée dans les statuts de l'ICANN[63]. Certes, les gouvernements ne se voient toujours pas reconnaître de rôle décisionnel, mais leur rôle consultatif est en revanche institutionnalisé grâce à la formation, au sein de l'institution, du «Governmental Advisory Comittee» (GAC)[64]. Comme son nom l'indique, ce «comité consultatif» n'a pas de pouvoir décisionnel ni exécutif dans l'ICANN: il rend des avis sur les dossiers que traite l'institution «*as they relate to concerns of governments, particularly matters where there may be an interaction between the Corporation's policies and various laws, and international agreements (or where they may affect public policy issues)*»[65], mais ne peut cependant théoriquement pas influer sur les décisions prises par le Bureau des Directeurs.

Tout en étant confiné dans son rôle purement consultatif, le GAC s'est néanmoins révélé au fil du temps être une émanation très nette des gouvernements nationaux, soucieux de légitimer les prétentions de ses membres à exercer l'autorité politique.

Ainsi, le principe général selon lequel «le système de nommage Internet est une ressource publique en ce sens que ses fonctions doivent être administrées dans l'intérêt public ou dans l'intérêt général»[66] a d'emblée été adopté par le GAC.

En 2000, dans ses principes de délégation et d'administration des domaines de premier niveau correspondant à des codes de pays[67], le GAC posa comme postulat que «*les gouvernements ou les autorités publiques sont responsables des objectifs de politique générale*» et en déduisit qu'«*au vu de leur responsabilité en matière de protection de ces intérêts, les gouvernements ou les autorités publiques conservent la responsabilité ultime en matière de politique ayant trait à leur(s) ccTLD(s) respectif(s)*»[68].

L'existence et l'évolution du GAC, entité «politique» par excellence, démontrent que les missions de l'ICANN ne se limitent pas à un simple rôle «technique». Au contraire, l'évolution de l'influence du GAC au sein de l'institution met en évidence la relation profonde entre «coordination technique» et «implications politiques», révélant ainsi que le champ de la gouvernance au sens strict n'est pas exempt de toute considération politique.

Pour illustrer cette considération, nous examinerons successivement les procédures d'inclusion, de délégation et de re-délégation de ccTLD, et relève-

63. Les statuts originaires de l'ICANN sont disponibles sur <http://www.icann.org/general/archive-bylaws/bylaws-23nov98.htm>. Ceux-ci ont été révisés à plusieurs reprises. Voy. <http://www.icann.org/general/corporate.html>.
64. Le GAC compte actuellement 100 membres, dont 40 sont des membres actifs. Il est ouvert aux représentants des gouvernements nationaux, chacun pouvant nommer un représentant et un conseiller pour siéger au Comité. Les économies distinctes reconnues dans les instances internationales, les organisations gouvernementales multinationales et les organisations régies par un traité peuvent également y adhérer sur invitation du président du GAC.
65. La participation du GAC dans les questions intéressant l'intérêt public n'était pas prévue dans les statuts originaires, mais a été rajoutée dans les statuts tels qu'amendés au 26 juin 2003.
66. GAC, *Principes de délégation et d'administration des domaines de premier niveau correspondant à des codes de pays*, 2000, disponible sur <http://www.icann.org/committees/gac/gac-cctldprinciples-23feb00.htm>.
67. *Ibid*.
68. *Ibid*.

rons les diverses retombées «politiques» que ces problématiques «techniques» ont sur le champ de la «gouvernance au sens strict».

2. L'inclusion de ccTLD dans le fichier-zone racine

Situés au niveau directement inférieur à la racine, les domaines de haut niveau correspondant à des codes pays (ccTLD) sont les zones qui auraient dû correspondre aux États selon le droit international public[69].

Néanmoins, lorsque la décision fut prise de créer un tel type de domaine, il a été convenu de prendre pour base des codes pays, la table ISO 3166-1 établie par l'*International Standardization Organization*.

Pour figurer sur la liste ISO 3166-1 gérée par l'*Autorité de mise à jour de l'ISO 3166*, et donc être considéré comme un code «acceptable» par l'ICANN, le nom doit soit être enregistré dans le «bulletin de terminologie Noms des pays»[70] publié par les Nations Unies, soit figurer dans la liste des «Codes des pays et des régions pour utilisation statistique»[71] maintenue par la Division de statistique des Nations Unies.

Malgré ses origines onusiennes, la table ISO 3166-1 reste cependant un code standard international utilisé pour représenter les entités géographiques, et non les États souverains. Ainsi, le Sahara occidental, Gibraltar ou Saint-Pierre-et-Miquelon disposent de leur propre ccTLD.

En conséquence, il existe beaucoup plus de ccTLD qu'il n'existe d'États. Par exemple, la France dispose de onze ccTLD différents, correspondant à des territoires tels que la Martinique, Mayotte, Wallis-et-Futuna ou la Nouvelle-Calédonie.

La référence à la norme ISO 3166-1 est souvent justifiée par le fait qu'il n'entre pas dans les compétences («techniques») de l'ICANN de décider quel territoire est un État et lequel n'en est pas un: le renvoi à la norme ISO 3166-1 poursuivrait ainsi un objectif de dépolitisation.

Relevons que cette considération est pour le moins amusante: tout en poursuivant un objectif de dépolitisation de l'institution, la référence à la norme ISO 3166-1 (et, par voie de conséquence, à certains documents de l'ONU) fait naître l'idée que l'inclusion d'un ccTLD dans la racine est en réalité une question éminemment politique. Plus piquant encore, l'admission d'un code pays dans le fichier-zone racine dépendrait, apparemment, de la reconnaissance d'un territoire par la communauté internationale.

De plus, les États associent de plus en plus leur ccTLD respectif à un élément représentatif de leur souveraineté. En atteste le fait que certains registres, comme par exemple ceux du Canada et des États-Unis, requièrent que le titulaire d'un nom de domaine soit établi dans l'État qu'il «représente», de telle manière que le nom de domaine de code pays devient une sorte de drapeau numérique auquel s'identifie la

69. G. CHATILLON, *op. cit.*, p. 4.
70. Afin d'être listé dans le «bulletin de terminologie Noms des pays», le territoire doit soit être un État membre des Nations Unies, soit être membre d'une agence spécialisée de l'ONU, soit être partie au Statut de la Cour Internationale de Justice.
71. Quant à la liste «Codes des pays et des régions pour utilisation statistique», celle-ci est basée sur le «bulletin de terminologie Noms des pays», ainsi que sur d'autres sources de l'ONU.

communauté nationale des titulaires de noms de domaine.

Le ccTLD devient donc petit à petit une «ressource nationale». Le Canada le décrit comme «*a key public resource, helping to promote the development of electronic commerce in Canada and important to our country's future social and economic development*»[72]. Le registre américain lui-même considère son ccTLD comme une «*national resource*»[73].

Par ailleurs, si la référence à la norme ISO 3166-1 est en théorie la ligne de conduite prônée par l'ICANN, en pratique cependant, l'institution privée, sous la tutelle du DoC, s'est écartée à plusieurs reprises de celle-ci en admettant l'inclusion dans le fichier-zone racine de codes pays non repris dans la liste officielle. La dimension politique est loin d'être absente dans ce domaine. Nous en livrons quelques exemples.

2.1. Le cas du .uk

La Grande-Bretagne est sans doute le premier État ayant bénéficié d'une exception au régime général de la référence à la norme ISO 3166. En effet, sur la liste officielle, la Grande-Bretagne est associée à l'extension .gb; pourtant, ce fut finalement l'extension .uk qui fut incluse dans le fichier-zone du serveur primaire de distribution.

Cette «bizarrerie» fut justifiée par des raisons techniques. L'extension .gb étant associée à l'époque à des noms de domaines JANET[74], il a été argué qu'il était plus facile de réaliser une transition entre les deux systèmes de nommage en associant une nouvelle extension à la Grande-Bretagne.

Il s'agit ici d'un premier degré d'interventionnisme ne respectant pas la ligne de conduite «dépolitisée» prônée par l'ICANN. Si, dans ce cas précis, une exception était tout à fait justifiable, elle n'en démontre pas moins l'importance du pouvoir de l'autorité «technique» de la racine: le pouvoir de modifier un drapeau numérique sans aucune reconnaissance préalable par la communauté internationale.

2.2. Le cas du .ps

En février 1997, la Palestine demanda à l'ICANN d'inclure le ccTLD «.ps» dans le fichier-zone du serveur primaire de distribution. À cette époque, aucun code n'était formellement associé à la Palestine dans la norme ISO 3166.

Cependant, en avril 1996, l'«Autorité de mise à jour de l'ISO 3166» intégra le code «ps» dans une liste réservée (catégorie «réservations exceptionnelles»), dont le but était de réserver le code alpha-2 «ps» pour la Palestine dans l'éventualité où elle serait incluse dans le futur dans la liste officielle de l'ISO 3166-1. En mai 1997, l'ICANN, respectant strictement sa ligne de conduite, refusa d'inclure le ccTLD «.ps» dans le fichier-zone racine du serveur primaire.

En été 1999, la Division de statistique des Nations Unies notifia à l'Autorité de mise à jour de l'ISO 3166 qu'elle avait intégré le nom «Territoire Palestinien Occupé» dans la liste des

72. K.G. von ARX et G.R. HAGEN, «Sovereign domains: A Declaration of Independence of ccTLDs from Foreign Control», *The Richmond journal of law and technology*, Volume IX, Issue 1, automne 2002, p. 11, disponible sur <http://law.richmond.edu/jolt/v9i1/Article4.html>.
73. *Ibid*.
74. JANET était le système d'adressage utilisé en Grande-Bretagne avant l'émergence de DNS.

Nations Unies des «Codes des pays et des régions pour utilisation statistique». En conséquence, le 30 septembre 1999, l'Autorité de mise à jour de l'ISO 3166 annonça qu'à dater du 1er octobre 1999, le code alpha-2 «ps» était associé au «Territoire Palestinien Occupé» dans la liste ISO 3166-1.

Ainsi, selon les lignes directrices de l'ICANN, l'extension put enfin être admise au sein du fichier-zone du serveur primaire. La Palestine a donc dû attendre pendant plus de deux ans pour voir son nom figurer au sein de la liste ISO 3166-1 officielle avant de pouvoir affirmer l'existence de son drapeau dans le monde numérique.

Au vu de l'affaire palestinienne, l'on peut évidemment se poser la question de la légitimité du critère de l'ISO 3166-1 pour baliser l'inclusion d'une extension dans le fichier-zone racine. En effet, dans le cadre du DNS, la reconnaissance par la «communauté internationale» a un effet tout à fait inédit: elle conditionne l'existence même d'un État dans le monde numérique.

Si, en droit international public, la controverse entre «*reconnaissance constitutive*» et «*reconnaissance déclarative*» existait bien entendu avant l'ère Internet, une grande nouveauté est cependant apportée au débat: jamais la reconnaissance d'un État par la communauté internationale n'avait eu pour effet de conditionner l'existence même de son territoire[75]!

2.3. Le cas du .eu

Par rapport au .ps, il est intéressant de relever la «différence de traitement» dont a bénéficié le code «eu» revendiqué par l'Union européenne. Tout comme l'était le code «ps», le code «eu» est en effet intégré uniquement dans la liste «intérim de réservation» de la division de statistique des Nations Unies; il n'apparaît nullement dans le bulletin de terminologie Noms des pays, ni dans la liste des Codes des pays et des régions pour utilisation statistique.

Toutefois, suite à une lettre du commissaire européen Erkki Liikanen, l'Autorité de mise à jour de l'ISO 3166 déclara «*(we have) decided to extend the scope of the reservation of the code element EU to cover any application of ISO 3166-1 that needs a coded representation of the name European Union, including its being used as an Internet Top Level Domain*»[76].

De manière très formelle, le code «eu» n'était donc pas inclus dans la liste officielle ISO 3166-1, de la même manière que «ps» ne l'était pas avant l'été 1999. Si la ligne directrice théorique de l'ICANN avait été suivie, il n'aurait donc pas été possible d'inclure l'extension .eu dans le fichier-zone racine. Or, celle-ci y fut incluse suite à une complexe résolution adoptée par le Bureau des Directeurs.

Les divergences entre les lignes de conduite dans le cadre des affaires européenne et palestinienne révèlent une inconsistance majeure de l'ICANN dans un domaine touchant à la souveraineté des États. Toute l'importance du contrôle des ressources techniques

75. Existence numérique.
76. ICANN minutes, *Special Meeting of the Board*, 25 septembre 2000, disponible sur <http://www.icann.org/minutes/minutes-25sep00.htm>.

DNS tombe ici sous le sens: il est en effet un outil potentiel de politique étrangère pour celui qui l'a entre ses mains.

3. La délégation et la re-délégation des ccTLD

3.1. Définition et principes de (re)-délégation

Une fois un code pays inclus dans le fichier-zone racine, encore faut-il que sa gestion soit assurée par quelqu'un, sans quoi l'existence d'un ccTLD n'aurait pas davantage d'effectivité que s'il n'existait pas. Lorsque l'on parle de délégation, c'est bien cette problématique qui est visée. La procédure de re-délégation vise, quant à elle, le changement de délégué, soit à l'initiative du gouvernement, soit à l'initiative de l'ICANN.

Le RFC 1591[77] est le premier document organisant les relations entre l'ICANN, les registres nationaux[78] et les gouvernements dans le cadre des questions de délégation et de re-délégation. Ce document est intéressant pour notre propos dans la mesure où il décrit le rôle fondamental de l'ICANN dans le cadre de la procédure de re-délégation: celui de s'assurer que le transfert de la gestion d'un ccTLD est réalisé avec l'accord mutuel de l'ancien et du nouvel administrateur, le but avoué étant d'éviter des re-délégations «politiques» pouvant menacer la stabilité du domaine.

Un document de l'ICANN[79] reprend les principes du RFC 1591. Il stipule également qu'en cas de conflit sur la désignation d'un administrateur de ccTLD, l'ICANN doit jouer un rôle de médiateur entre les différentes parties afin de parvenir à un accord[80]. Généralement, l'ICANN n'a donc qu'un rôle passif dans la désignation des délégués. Ce n'est que lorsqu'un accord mutuel ne peut être atteint que l'ICANN devrait avoir un rôle plus actif dans le processus. À nouveau, le souci d'assurer la stabilité de DNS et d'éviter les re-délégations «politiques» semble justifier la mesure.

Le GAC a également publié un document essentiel concernant les Principes de délégation et d'administration des domaines de premier niveau correspondant à des codes de pays[81] visant à encourager l'élaboration de bonnes pratiques concernant la délégation et l'administration des ccTLD. Il n'a pas force de loi, mais le GAC a invité les différents gouvernements à adhérer à ces principes. Ceux qui déclarent s'y soumettre les adoptent *de facto* comme des règles organisant leurs relations avec l'ICANN comme avec leur délégué national[82]. Selon ce document, une re-délégation est possible selon certaines conditions, soit à l'initiative du gouvernement, soit à l'initiative de l'ICANN.

77. Le texte est disponible sur <http://www.faqs.org/rfcs/rfc1591.html>.
78. Les registres nationaux sont des personnes juridiques à qui l'ICANN délègue la gestion d'un ccTLD. Les registres nationaux ont des personnalités juridiques diverses: entreprise privée, comme aux États-Unis, au Japon, en Ukraine, en Gambie, associations, comme à l'intérieur de nombreux pays de l'Union européenne (dont la France), institutions indépendantes de l'État, comme en Suisse ou en Colombie, ou encore organismes totalement intégrés à l'appareil étatique, comme en Inde, en Espagne, en Argentine ou en Finlande.
79. ICANN, *ICP-1: Internet Domain Name System Structure and Delegation, ccTLD Administration and Delegation*, 1999, disponible sur <http://www.icann.org/icp/icp-1.htm>.
80. *Ibid.*
81. GAC, *Principles for Delegation and Administration of ccTLDs*, 23 février 2000, disponible sur <http://www.icann.org/committees/gac/gac-cctldprinciples-23feb00.htm>.
82. En 2000, la Commission européenne a d'ailleurs recommandé aux États européens d'adhérer à ces principes et à les mettre en œuvre. Voy. *L'organisation et la gestion de l'Internet. Enjeux internationaux et européens 1998-2000*, Communication de la Commission, COM(2000) 202 final du 11 avril 2000, p. 17.

Tout d'abord, le gouvernement, pour prendre l'initiative d'une re-délégation, doit démontrer à l'ICANN que le délégué a enfreint les règles ou que son mandat a expiré. L'ICANN réaffecte alors la délégation en accord avec le gouvernement. Cette règle fixe le cadre du pouvoir d'un gouvernement sur son registre: le gouvernement doit pouvoir prouver que le délégué a commis un manquement aux règles précisées dans le contrat l'unissant à lui. Si aucun contrat n'existe, la réaffectation peut être opérée selon une procédure analogue, mais le gouvernement doit alors prouver que le registre «*n'a pas son soutien ni celui de la communauté locale concernée, ou qu'il a enfreint d'autres dispositions essentielles du RFC 1591 et qu'il a négligé d'y porter remède*».

Ces conditions rendent complexe toute procédure de réaffectation d'une délégation déjà existante à l'initiative des gouvernements nationaux. L'objectif de la mesure étant, sans aucun doute, de protéger les délégués de l'arbitraire de leurs gouvernements respectifs et de leur assurer une certaine stabilité à l'abri des contingences politiques nationales.

Quant à l'ICANN, l'organisation peut demander à un gouvernement de procéder à une réaffectation de la délégation si elle considère que «*le ccTLD est exploité d'une manière qui menace la stabilité du DNS ou d'Internet ou si il est exploité en infraction avec d'autres dispositions matérielles du contrat entre l'ICANN et le délégué*». Dans ce cas, l'ICANN peut demander au gouvernement concerné de désigner un nouveau délégué. La raison fondamentale pour laquelle une re-délégation est possible à l'initiative de l'ICANN étant le manquement du délégué à ses obligations contractuelles, l'organisation tente à présent de remédier au manque de formalisme[83] en incitant les administrateurs de ccTLD à entrer en relation contractuelle avec elle. Ainsi, le 25 septembre 2000, le Bureau des Directeurs adopta une résolution[84] par laquelle il requit qu'un accord contractuel soit passé entre le registre et l'ICANN avant toute nouvelle délégation de ccTLD[85]. Depuis cette résolution, un nombre croissant de «contrats de délégation»[86] (*sponsorship agreements*) sont négociés avec fruit entre registres et l'ICANN[87]. À notre connaissance, tous les ccTLD re-délégués depuis lors ont en effet fait l'objet d'un tel contrat, à deux exceptions près: le .ca (Canada) et le .us. Ces contrats sont des accords d'une importance primordiale dans le contexte hiérarchisé du DNS. C'est en effet par ceux-ci que l'autorité suprême de la racine délègue une portion d'autorité administrative aux registres nationaux. Leur respect étant de toute évidence assuré grâce à la sanction potentielle de la «re-délégation», l'on comprend aisément que les dispositions contractuelles influenceront sans aucun doute les politiques locales décidées au niveau de chaque registre national. Il s'agit là d'une des conséquences de l'«administration sur le modèle technique» et de la «régulation en cascade».

Si, selon les documents examinés, les considérations politiques doivent rester étrangères en matière de re-délé-

83. À l'origine, les ccTLD étaient délégués par Jon POSTEL sans aucun accord formel écrit.
84. ICANN, *Preliminary Report, Special Meeting of the Board*, 25 septembre 2000, disponible sur <http://www.icann.org/minutes/prelim-report-25sep00.htm>).
85. Cette formalité s'impose également lors de la re-délégation d'un ccTLD existant à un nouveau registre.
86. Ces contrats spécifient, entre autres, la contribution financière que le registre doit verser à l'ICANN et les conditions dans lesquelles l'ICANN et le registre peuvent résilier le contrat, d'autres clauses étant imaginables.
87. Tel fut le cas notamment de l'Australie, du Japon, du Malawi, du Burundi, de l'Ouzbekistan et de l'Union européenne.

gation, l'actualité démontre cependant que cette ligne de conduite n'est pas toujours respectée avec la même rigueur. Afin d'illustrer ceci, nous examinons quelques cas pratiques de réaffectation.

3.2. Le cas du .ph[88]

Début 2005, le gouvernement des Philippines a réclamé de façon assez virulente dans la plupart des forums internationaux le contrôle du .ph, détenu – comme c'est souvent l'usage – par des ingénieurs qui en assuraient la gestion bien avant que le gouvernement ne s'intéresse à la notion même d'Internet. Ces ingénieurs ont décidé de combattre, d'une façon assez originale, l'idée selon laquelle le gouvernement serait mieux qualifié qu'eux pour gérer le ccTLD. Le sous-domaine .gov.ph étant géré directement par les services du gouvernement, qui pouvaient être amenés à gérer le .ph en entier si la re-délégation avait bien lieu, les opérateurs actuels se sont amusés à comparer leur taux d'efficacité avec celui du gov.ph… Les résultats[89] de cette étude se sont révélés catastrophiques pour le gouvernement philippin. La re-délégation n'eut pas lieu.

Cette affaire reflète le principe selon lequel une re-délégation à l'initiative du gouvernement ne peut avoir lieu pour une simple raison d'opportunité politique, la stabilité «technique» devant rester la préoccupation principale.

3.3. Le cas du .us

Le 26 octobre 2001, le gouvernement américain conclut un accord avec Neustar Inc., le chargeant de la gestion du ccTLD .us, géré à cette époque par VeriSign. Ce transfert eut lieu en contradiction totale avec la politique de l'ICANN et avec les principes inscrits dans le RFC 1591 et ICP-1, requérant un accord mutuel entre l'ancien et le nouveau registre. De plus, la re-délégation eut lieu en l'absence de «contrat de re-délégation» conclu avec l'ICANN.

Lors de cette réaffectation, le gouvernement des États-Unis informa en effet l'ICANN que «*because of complexities of U.S. procurement laws, it was not able to extend the existing arrangements with VeriSign nor complete the necessary three-way set of communications among itself, ICANN, and NeuStar*»[90].

L'ICANN expliqua par la suite que si elle n'avait pas accepté la re-délégation à l'initiative du gouvernement, cela aurait créé «*a situation where the event would have occurred regardless but there would be inconsistent data in the IANA database*»[91].

En d'autres mots, l'ICANN n'ayant pas le pouvoir d'empêcher le gouvernement des États-Unis de modifier le contenu au sein du serveur racine primaire, elle n'avait pas le pouvoir d'empêcher la re-délégation technique du .us. Compte tenu de sa mission première, qui consiste à assurer la stabilité technique de l'Internet, elle a donc été obligée de faire concorder les informations

88. «Vie des extensions : .PH : Faire honte au gouvernement pour empêcher une redélégation !», *Domaine.info*, Newsletter n° 23, 18 mars 2005, disponible sur <http://www.domaine.info/archives/news/23_20050318/extension/news_20050318_5.html>.
89. Les résultats de l'enquête sont disponibles sur <http://jed.i.ph/lesspolitics(21x24).pdf>.
90. ICANN Announcement, *Redelegation of .us Country-Code Top-Level Domain*, 19 novembre 2001, disponible sur <www.icann.org/announcements/announcement-19nov01.htm>.
91. *Ibid.*

juridiques relatives au délégué avec les informations entrées dans le serveur primaire par le DoC[92].

Cette affaire illustre le fait que le contrôle technique de l'infrastructure dont dispose le gouvernement des États-Unis, par le biais de l'accord avec VeriSign, a des répercussions concrètes sur la gestion du fichier-zone racine. De plus, l'argument soulevé dans ce contexte par le gouvernement américain (« *because of complexities of U.S. procurement laws…* ») met en lumière le fait que les arguments politiques ont leur place dans le débat de la gestion des ccTLD.

Plus généralement, le cas du .us révèle que, dans certaines circonstances, une re-délégation peut concrètement avoir lieu pour un motif purement politique, en contradiction totale avec les principes fixés par le GAC et le RFC 1591, et qu'un « contrat de délégation » n'est pas toujours requis.

3.4. Le cas du .ht[93]

Depuis sa création en 1997, le .ht, ccTLD d'Haïti, était géré de manière artisanale par un « ami » de Jon Postel[94], qui, en ces temps préhistoriques pour le réseau, avait tendance à attribuer la gestion d'une extension à ceux qu'il sentait dignes de confiance.

En mars 2002, un consortium formé à l'initiative du Réseau de Développement Durable d'Haïti (RDDH) et soutenu par le gouvernement haïtien a demandé à l'ICANN de lui confier la gestion du .ht. La démarche du nouveau gestionnaire haïtien semblait aussi logique que censée. Le .ht n'avait en effet jamais fonctionné. Le gouvernement et les spécialistes de ce pays ont donc souhaité en reprendre la gestion pour enfin lui donner vie.

Ce qui gêne dans ce dossier, c'est le temps de délibération de l'ICANN: il aura fallu attendre deux ans pour qu'enfin le .ht soit re-délégué. Rappelons qu'il n'a fallu qu'un mois au gouvernement US pour obtenir l'aval de l'ICANN concernant la re-délégation de son ccTLD en 2001. Suite à cette affaire, l'ICANN a été accusée de faire du chantage auprès des « petites » extensions en traînant les pieds lors des questions de re-délégation[95]. Le but: obtenir la signature d'un « contrat de délégation » dont on a déjà examiné les implications au niveau de la « régulation en cascade ».

Les administrateurs qui acceptent d'entrer en relation contractuelle avec l'ICANN semblent obtenir gain de cause rapidement, les autres pouvant parfois attendre longtemps. Dans le cas du .ht, les autorités haïtiennes, *a priori* peu favorables à la signature de ce contrat, auraient finalement accepté.

3.5. Le cas du .af[96]

Avant la chute du régime taliban, l'extension .af ne « fonctionnait » plus depuis longtemps. Les Talibans avaient bien entendu banni l'Internet, mais même avant leur arrivée, le cyberespace national afghan avait été fort

92. K.G. von ARX et G.R. HAGEN, *op. cit.*, p. 13.
93. IANA, *Report on Redelegation of the .ht Top-Level Domain*, janvier 2004, disponible sur <http://www.iana.org/reports/ht-report-13jan04.htm>.
94. Jon POSTEL fut l'un des principaux contributeurs à la création de l'Internet. Il est le premier membre de l'Internet Society et était le responsable de l'IANA.
95. Domain News, *.HT: Une redélégation politique,* 5 février 2004, disponible sur <http://www.domaine.info/archives/news/13_20040205/gouv/news_20040205_1.html>.
96. IANA, *Report on Redelegation of the .af Top-Level Domain*, *op.cit.*

maltraité. En 1997, c'est un certain Abdul Razeeq qui avait demandé à l'ICANN de lui confier la gestion du .af. L'individu avait cependant vite disparu, laissant donc un pays sans son extension.

Avec la chute des Talibans, les Nations Unies et le gouvernement afghan ont entamé une action commune pour faire renaître le .af. «*C'est une part de notre souveraineté que nous venons de récupérer*», s'est félicité Mohammad Moassom Stanakzai, le ministre de la Communication afghan. Et l'ONU d'ajouter, par le biais d'un communiqué officiel: «*L'Afghanistan reprend ainsi le contrôle juridique et technique de son espace Internet*». Ce furent donc des arguments de souveraineté qui furent invoqués dans le cadre de cette procédure pour justifier le transfert de la gestion du .af au ministre des Communications du «Gouvernement islamique transitoire» au pouvoir à Kaboul[97].

Dans ce dossier, outre le fait que la re-délégation ait été faite au bénéfice de la nouvelle autorité politique afghane, ce qui étonne, c'est la rapidité avec laquelle la procédure de re-délégation fut menée à son terme. En effet, en septembre 2002, le ministre des Communications fit parvenir la requête de re-délégation à l'ICANN, et quatre mois plus tard, en janvier 2003, la procédure était déjà clôturée, un «contrat de délégation»[98] ayant été rapidement accepté par le nouveau délégué.

4. La gestion de la racine, une question «politique»

Après avoir examiné ces quelques cas pratiques d'inclusion et de re-délégation, il semble à tout le moins évident que les considérations politiques ne sont pas totalement étrangères au jugement effectué par l'ICANN dans sa gestion de la racine. Ce constat démontre, selon nous, que la division technico-politique prônée par le DoC est loin d'être aussi étanche qu'on aurait pu l'imaginer de prime abord. En effet, nous avons pu remarquer que les gouvernements nationaux, la communauté Internet globale et le DoC sont susceptibles d'avoir des intérêts divergents quant à l'inclusion d'un ccTLD et à l'identité du registre finalement retenu.

En matière de re-délégation, si la référence à la norme ISO 3166 et les principes du document ICP-1 reflètent une position louable tendant à dépolitiser la gestion du DNS afin de faire primer la stabilité technique sur l'«insécurité politique», dans les faits, une telle position n'est tenable que si l'ensemble des gouvernements, y compris celui des États-Unis, sont respectueux de ces lignes de conduite.

Le droit de veto accordé au DoC sur l'édition du fichier-zone racine, ainsi que les «contrats de délégation», ont donc assurément des répercussions politiques. Admettre que dans le cadre des procédures d'inclusion et de re-délégation, et donc du débat relatif à la «gouvernance au sens strict», la dimension politique est loin d'être absente, conforte l'idée qu'une place de choix devrait être réservée aux autorités nationales concernées et aux arguments

97. Selon certains, le gouvernement américain aurait re-délégué l'extension à l'ONU par le truchement du gouvernement de transition. Voy. C. DELACOURT, «Les noms de domaine, enjeu de la géopolitique américaine», *ZDNet*, 6 mai 2003, disponible sur <http://www.zdnet.fr/actualites/imprimer/0,50000200,2134301,00.htm>.

98. ICANN, *.af ccTLD Memorandum of Understanding*, 8 janvier 2003, disponible sur <http://www.icann.org/cctlds/af/mou-08jan03.htm>.

de souveraineté (*cf.* affaires du .ht et du .af).

Non seulement l'existence même d'un État dans le monde numérique se trouve fragilisée par le fait que toute décision d'ajout ou de suppression d'un ccTLD doit être approuvée par le DoC, mais l'on peut d'ores et déjà aisément imaginer les implications qu'un tel contrôle centralisé peut avoir sur la sécurité nationale des États autres que les États-Unis.

À l'heure de l'Internet, bon nombre de services nationaux sont en effet disponibles «on-line». En temps de guerre ou de conflit économique, il est évident que la désactivation d'une zone serait une aubaine pour l'État ayant le contrôle de l'infrastructure. Ceci sera d'autant plus vrai lorsque la téléphonie sur IP (VOIP)[99] se substituera à la téléphonie classique en commutation par circuit[100]. Le contrôle du serveur racine primaire deviendrait ainsi d'un grand intérêt stratégique, permettant potentiellement de mettre à mal l'un des grands moyens de communication de l'«ennemi».

Bill Clinton lui-même, fervent défenseur de l'«autorégulation» à la mode US, était tout à fait conscient de la nécessité d'un contrôle de l'infrastructure en déclarant que «*The United States possesses both the world's strongest military and its largest national economy. Those two aspects of our power are mutually reinforcing and dependent. They are also increasingly reliant upon certain critical infrastructures and upon cyberbased information system*»[101].

L'Union européenne semble comprendre les risques qu'une centralisation technique des ressources peut avoir sur l'effectivité de l'autorité politique des États (autres que les États-Unis). Dès le 18 juin 2002[102], l'Union européenne a ainsi suggéré que le DoC abandonne son pouvoir de contrôle unique sur le serveur primaire au profit du GAC ou d'un autre organisme international, prônant ainsi pour une certaine internationalisation du contrôle technique.

Cependant, il est peu probable que le DoC acquiesce un jour à de telles revendications. Le 30 juin 2005, peu avant le Sommet de Tunis, le DoC a en effet rappelé que:

«*The United States Government intends to preserve the security and stability of the Internet's Domain Name and Addressing System (DNS). Given the Internet's importance to the world's economy, it is essential that the underlying DNS of the Internet remain stable and secure. As such, the United States is committed to taking no action that would have the potential to adversely impact the effective and efficient operation of the DNS and will therefore maintain its historic role in authorizing changes or modifications to the authoritative root zone file*»[103].

Tout en gardant en mémoire cette déclaration de principe du DoC, exami-

99. «Voice over IP» est le terme anglais décrivant le transport de la voix sur réseau Internet. Le principe est de transformer et de compresser la voix en données numériques et de les acheminer jusqu'au destinataire dans de simples paquets TCP/IP.
100. En effet, le DNS est utilisé par le protocole ENUM, qui permet de créer des noms de domaine à partir des numéros de téléphone et de les associer à des services de communication.
101. «The Clinton Administration Policy on Critical Infrastructure Protection», Presidential Decision Directive 63, 22 mai 1998, disponible sur <http://www.fas.org/irp/offdocs/paper598.htm>.
102. EU Telecommunications Council, «Guidelines for discussion», 18 juin 2002, disponible sur <http://www.icannwatch.org/article.pl?sid=02/06/21/125909&mode=thread>.
103. United States Department of commerce, NTIA, *Domain Names: U.S. Principles on the Internet's Domain Name and Addressing System*, *op. cit.*

nons à présent «la gouvernance de l'Internet» telle qu'elle fut définie par le GTGI et les conséquences de cette définition sur l'issue du Sommet de Tunis.

Chapitre 4
La gouvernance au sens strict suite au SMSI

1. L'amalgame entre «gouvernance au sens strict» et questions techniques

Dans notre introduction, nous avions déjà mentionné le caractère extrêmement large de la définition de «gouvernance de l'Internet» élaborée par le Groupe de travail sur la gouvernance de l'Internet (GTGI) lors de la première phase du Sommet mondial sur la société de l'information (SMSI).

Le GTGI ayant été conçu en tant que «*groupe de travail chargé de préparer le terrain pour les négociations de la phase de Tunis*»[104], on ne s'étonnera pas de retrouver la même envergure conceptuelle dans *l'Agenda de Tunis pour la société de l'information*, l'un des résultats finaux du Sommet mondial[105].

Ainsi, au point 58, l'Agenda reconnaît «*que la gouvernance de l'Internet va au-delà des questions de nommage et d'adressage. Elle recouvre aussi des questions de politique publique importantes comme les ressources Internet essentielles, la sécurité et la sûreté du réseau, des aspects touchant au développement et des questions se rapportant à l'utilisation de l'Internet*». À l'issue du SMSI, le champ de la gouvernance de l'Internet couvre donc aussi bien des considérations touchant à la «gouvernance au sens strict» que des questions touchant à la «gouvernance au sens large».

Parallèlement, l'étendue de ce champ d'application s'accompagne d'une réitération de la distinction classique entre questions techniques et considérations politiques. Le point 35 de l'Agenda réaffirme ainsi «*que la gestion de l'Internet couvre aussi bien des questions d'ordre technique que des questions de politique générale*».

De cette distinction hasardeuse, dont les limites ont déjà été démontrées, découle le rôle des gouvernements nationaux. Selon le point 69 de l'Agenda, ceux-ci ne devraient s'acquitter d'aucun «*rôle*» ni d'aucune «*responsabilité*» dans les «*questions techniques et opérationnelles courantes qui n'ont pas d'incidence sur les questions de politique publique internationale*». Par contre, «*en ce qui concerne les questions d'intérêt général qui se rapportent à l'Internet, le pouvoir décisionnel relève de la souveraineté nationale des États, lesquels ont des droits et des responsabilités en la matière*».

104. GTGI, *Rapport préliminaire du Groupe de Travail sur la Gouvernance de l'Internet*, ref WSIS-II/PC-2/DOC/5-F, 21 février 2005, disponible sur <http://www.itu.int/wsis/docs2/pc2/off5-fr.doc>, p. 3.

105. «*Une définition de la gouvernance de l'Internet est l'élaboration et l'application par les États, le secteur privé et la société civile, chacun selon son rôle, de principes, normes, règles, procédures de prise de décision et programmes communs propres à modeler l'évolution et l'utilisation de l'Internet*» (Agenda de Tunis pour la société de l'information, WSIS-05/TUNIS/DOC/6 (rev. 1), 18 novembre 2005, pt 34, disponible sur <http://www.itu.int/wsis/docs2/tunis/off/6rev1-fr.html>).

Dans le même esprit, Kofi Annan, le secrétaire général des Nations Unies, déclara: «*Soyons clairs: les Nations Unies ne veulent pas reprendre l'Internet ni ne veulent le contrôler comme un pouvoir politique. La gestion quotidienne de l'Internet doit être confiée à des institutions techniques, ne fût-ce que pour le protéger des échauffements de la politique au quotidien*»[106].

Selon nous, l'amalgame se situe ici: le champ de la «gouvernance au sens strict» serait par essence «technique», tandis que celui de la «gouvernance au sens large» serait, par nature, «politique». Par conséquent, si le rôle des gouvernements se situerait essentiellement en matière de gouvernance au sens large, il serait nettement plus atténué dans le champ de la gouvernance au sens strict.

Si l'Agenda reconnaît toutefois «*la nécessité d'une coopération*» visant à «*favoriser la création d'un environnement qui facilite l'élaboration de principes applicables à la coordination et la gestion des ressources fondamentales de l'Internet*»[107], les acteurs de cette coopération devront cependant être les «*organisations internationales compétentes*» – lisez l'ICANN –, et non les gouvernements.

2. Les conséquences du SMSI sur la répartition des compétences en matière de gouvernance au sens strict au niveau de la racine

L'un des résultats concrets du SMSI fut sans aucun doute la création d'un nouveau forum destiné à établir un dialogue entre les multiples parties prenantes sur les politiques à suivre dans le cadre de la «gouvernance». Il s'agit du *Forum sur la gouvernance de l'Internet* (FGI)[108].

Le FGI, dans son fonctionnement et sa fonction, devrait «*avoir un caractère multilatéral, multi-parties prenantes, démocratique et transparent*» et «*s'inspirer des structures existantes de gouvernance de l'Internet, l'accent étant mis en particulier sur la complémentarité entre toutes les parties prenantes participant à ce processus (gouvernements, entités du secteur privé, société civile et organisations intergouvernementales)*».

Le mandat du FGI comporte notamment le traitement «*des questions relatives aux ressources fondamentales de l'Internet*». Cependant, il importe de noter que «*le Forum n'aurait aucune fonction de contrôle et ne remplacerait pas les mécanismes, institutions ou organisations existants mais les ferait intervenir et s'appuierait sur leurs compétences. Il constituerait un mécanisme neutre, ne faisant pas double emploi et non contraignant. Il n'interviendrait pas dans les opérations courantes ou techniques de l'Internet*»[109].

Selon l'Agenda, il existerait ainsi une distinction claire entre les «*questions relatives aux ressources fondamentales de l'Internet*» et les «*opérations courantes ou techniques de l'Internet*»[110], confirmant ainsi l'amalgame entre «gouvernance au sens strict» et «considérations techniques». De plus, l'ICANN étant en charge de ces «*opérations courantes ou techniques de l'Internet*», et afin de ne pas faire double emploi, l'Agenda

106. M. MOORE, «World Conference: Grumbling Continues Over Internet Control», *Associated Press*, 17 novembre 2005.
107. Agenda de Tunis pour la société de l'information, *op. cit.*, pt 70.
108. *Ibid.*, pt 72.
109. *Ibid.*, pt 73.
110. *Ibid.*, pt 69.

n'attribue aucune compétence en matière de gouvernance au sens strict au FGI.

Par conséquent, en recommandant de se baser sur les «*mécanismes, institutions ou organisations existants*»[111], l'Agenda maintient le *statu quo* au niveau de la racine. En effet, même si l'organisation n'est pas nommée spécifiquement dans l'Agenda, l'ICANN demeure en charge de la gouvernance au sens strict au niveau hiérarchique suprême.

À l'issue du SMSI, l'influence des autorités politiques nationales en matière d'adressage et de nommage ne pourra donc s'exprimer, tout au plus, que par l'intermédiaire du GAC, organe consultatif au sein de l'ICANN.

Plus fondamentalement, le tissu contractuel assurant au DoC le contrôle politique et administratif sur la racine reste inchangé. Les objectifs et priorités en matière de gestion et de coordination des ressources fondamentales de l'Internet continueront à être déterminés dans le cadre de la «corégulation transitoire» organisée par le MoU. Dans le même esprit, les procédures et politiques qui guident l'exercice des fonctions IANA, et donc *in fine* les principes d'inclusion et de re-délégation, continueront à être définies par le DoC. Enfin, par l'effet de l'accord de coopération avec VeriSign, le DoC maintient son droit de veto sur l'édition du fichier-zone racine, et reste donc l'unique titulaire d'un pouvoir de contrôle sur la ressource fondamentale de DNS.

La volonté du DoC de «*maintenir son rôle historique*»[112] dans les procédures d'édition du fichier-zone racine a donc été largement respectée. Bien que toute position politique raisonnée et saine rejette à juste titre une gestion unilatérale du DNS, les participants du SMSI ont attentivement écouté, à Tunis, les contre-arguments des techniciens américains. Leur crainte selon laquelle une lutte de pouvoir politique menacerait la stabilité technique de l'Internet a été plus qu'entendue. En témoigne le nombre de références faites par l'Agenda à l'importance de la «*sécurité*» et de la «*stabilité*» de l'Internet[113]; les mêmes arguments qui avaient été utilisés par le DoC dans sa déclaration de principe du 30 juin 2005.

Au final, en ce qui concerne le contrôle des ressources fondamentales, l'Agenda de Tunis n'énonce qu'un vœu pieux selon lequel:

«*Nous reconnaissons que tous les gouvernements devraient avoir égalité de rôle et de même responsabilité dans la gouvernance internationale de l'Internet ainsi que dans le maintien de la stabilité, de la sécurité et de la continuité de ce réseau. Nous reconnaissons également la nécessité pour les gouvernements d'élaborer des politiques publiques en consultation avec toutes les parties prenantes*»[114].

L'avenir seul pourra nous révéler si cette profession de foi connaîtra, un jour, une matérialisation.

111. *Ibid.*, pt 73.
112. United States Department of commerce, NTIA, *Domain Names: U.S. Principles on the Internet's Domain Name and Addressing System*, *op. cit.*
113. Voy. Agenda de Tunis pour la société de l'information, *op. cit.*, pts 45, 57 et 68.
114. *Ibid.*, pt 68.

3. Les conséquences du SMSI sur la répartition des compétences en matière de gouvernance au sens strict au niveau des ccTLD

En ce qui concerne les ccTLD, l'Agenda précise, au point 68, que «*les pays ne devraient pas intervenir dans des décisions relatives au domaine de premier niveau correspondant au code de pays (ccTLD) d'un autre pays. Les intérêts légitimes nationaux, tels qu'ils sont exprimés et définis par chaque pays, de diverses manières, en ce qui concerne les décisions relatives à leurs ccTLD doivent être respectés, défendus et traités dans un cadre et au moyen de mécanismes souples et améliorés*».

Selon l'Agenda, les «*intérêts nationaux*» auraient donc une place prépondérante dans les décisions relatives au domaine de premier niveau correspondant à des codes de pays.

Toutefois, compte tenu des effets déjà mentionnés du «contrôle unilatéral des ressources», de la «régulation en cascade», des «contrats de délégation» et du rôle consultatif du GAC au sein de l'ICANN, il importe de relativiser cette déclaration, de la même manière que nous avions relativisé l'exception, incluse dans le *White Paper*, selon laquelle «*National governments acting as sovereigns… should (not) participate in management of Internet names and addresses (but will) continue to have, authority to manage or establish policy for their own ccTLDs*»[115].

De manière similaire, si l'Agenda réaffirme la responsabilité de politique générale des gouvernements nationaux en ce qui concerne leurs ccTLD respectifs, il ne faudrait cependant pas perdre de vue les conséquences du contrôle unilatéral du DoC sur le fichier-zone racine.

En effet, si l'Internet est par définition mondial, le DNS en est cependant le point de contrôle. Il en résulte une situation absurde: des États tentent d'affirmer leur autorité de manière abstraite sans en avoir les moyens concrets. Tout en essayant d'affirmer leur autorité en matière de «gouvernance au sens large», les États, autres que les Etats-Unis, sont, en effet, privés du contrôle de fait d'un élément clé de leur souveraineté nationale. L'existence même de l'«État» dans le monde numérique se trouve ainsi laissée au pouvoir de fait d'un gouvernement étranger; ne reste aux gouvernements nationaux qu'une «autorité» purement rhétorique dont le champ est plus qu'énigmatique. Il ne peut, selon nous, y avoir d'autorité effective sans contrôle des ressources.

Conclusion

Selon nous, le maintien d'une distinction claire entre «gouvernance au sens strict» et «gouvernance au sens large» aurait permis de clarifier les débats lors du Sommet mondial sur la société de l'information.

Tout d'abord, pour une raison très concrète. Avant le SMSI et la mise en place du *Forum sur la gouvernance de l'Internet*, il n'existait, en effet, ni structures ni mécanismes formels en charge du champ de la «gouvernance au sens

115. *Ibid.*

large». De plus, étant donné la quantité de matières appelées à être débattues, l'on pouvait raisonnablement s'attendre à des négociations longues et houleuses. Un résultat acceptable par l'ensemble des participants ne pouvait donc être attendu qu'à moyen ou long terme.

En ce qui concerne «la gouvernance au sens strict» par contre, la thématique était clairement définie dès le départ. Par ailleurs, les structures institutionnelles, mécanismes et procédures avaient déjà été mis en place de longue date. Même si la matière promettait une lutte politique acharnée, l'issue aurait donc pu être examinée à plus court terme.

De ce point de vue, la juxtaposition des questions relatives au nommage et à l'adressage avec les problématiques de «gouvernance au sens large» (cybercriminalité, *spam*, propriété intellectuelle, liberté d'expression, multilinguisme, droit des consommateurs, protection de la vie privée, concurrence, lutte contre la fracture numérique, *etc.*) a rendu le Sommet quelque peu fourre-tout. «Gouvernance au sens strict» et «gouvernance au sens large» auraient dû être examinées, chacune, dans leur spécificité propre pour faire l'objet de discussions circonstanciées et de politiques distinctes. Peut-être ceci aurait-il permis, très concrètement, de sortir de l'impasse.

Ensuite, pour une raison plus méthodologique. Une séparation entre «transmission» et «contenu» au niveau du débat général sur la gouvernance aurait, selon nous, permis de structurer plus intelligiblement l'élaboration des politiques dans l'Agenda de Tunis. L'on sait que, de manière générale en Europe, la réglementation de la transmission[116] est séparée de celle des contenus. Une ligne de démarcation analogue entre problématiques de «gouvernance au sens strict» et «gouvernance au sens large» aurait eu l'avantage, à nouveau, de tenir compte des spécificités de chacune de ces questions, tout en permettant d'identifier plus distinctement les liens entre celles-ci. Les textes finaux en auraient, sans doute, gagné en clarté.

Enfin, pour une raison purement «politique». Rappelons en effet que l'Agenda de Tunis est basé sur le principe selon lequel «*l'Internet est devenu une ressource publique mondiale et sa gouvernance devrait constituer l'une des priorités essentielles de la société de l'information*».

Étant donné que la répartition de compétences en matière de «gouvernance au sens strict» détermine l'effectivité des mécanismes de «gouvernance au sens large», il aurait été préférable de distinguer les deux aspects afin que «la gestion internationale de l'Internet» puisse «*s'opérer de façon multilatérale, transparente et démocratique, avec la pleine participation des États, du secteur privé, de la société civile et des organisations internationales et assurer une répartition équitable des ressources*»[117].

116. Voy. le cadre réglementaire des communications électroniques mis en place par la Dir. 2002/21/CE du Parlement européen et du Conseil, du 7 mars 2002, relative à un cadre réglementaire commun pour les réseaux et les services de communications électroniques (directive «cadre»), et plus particulièrement le consid. 5 de cette directive.
117. Agenda de Tunis pour la société de l'information, *op. cit.*, pt 29.